Lecture 8
Primitive Roots (Prime Powers), Index Calculus

Recap - if prime p, then there's a primitive root g mod p and it's order mod p is $p-1 = q_1^{e_1} q_2^{e_2} \dots q_r^{e_r}$. We showed that there are integers g_i mod p with order exactly $q_i^{e_i}$ (counting number of solutions to $x^{q_i^{e_i}} - 1 \equiv 0 \bmod p$). Set $g = \prod g_i$ - has order $\prod q_i^{e_i} = p-1$.

Number of primitive roots - suppose that m is an integer such that there is a primitive root g mod m. How many primitive roots mod m are there?

We want the order to be exactly $\phi(m)$. If we look at the integers 1, g, g^2, $\dots g^{\phi(m)-1}$, these are all coprime to m and distinct mod m. If we had $g^i \equiv g^j$ mod m ($0 \leq i < j \leq \phi(m)-1$), then we'd have $g^{j-1} \equiv 1$ mod m with $0 \leq j - i < \phi(m)$, contradicting the fact that g is a primitive root.

Since there are $\phi(m)$ of these integers, they must be all the reduced residue classes mod m (in particular if $m = p$, a prime, then $\{1, 2, \dots p-1\}$ is a relabeling of $\{1, g, \dots g^{p-2}\}$ mod p). Suppose that a is a primitive root mod m, then $a \equiv g^k$ mod m. Recall that order of g^k is

$$\frac{\mathrm{ord}(g)}{(k, \mathrm{ord}(g))} = \frac{\phi(m)}{(k, \phi(m))}$$

So only way for the order to be exactly $\phi(m)$ is for k to be coprime to $\phi(m)$. Ie., the number of primitive roots mod m is exactly $\phi(\phi(m))$ - if there's at least one. In particular, if $m =$ a prime, then number of primitive roots is $\phi(p-1)$.

Conjecture 37 (Artin's Conjecture)**.** *Let a be a natural number, which is not a square. Then there are infinitely many primes p for which a is a primite root mod p.*

This is an open question. Hooley proved this conditional on GRH, and Heath-Brown showed that if a is a prime, then there are at most 2 values of a which fail the conjecture

(Definition) Discrete Log: Say p is a prime, and g is a primitive root mod p (ie., $1, g, g^2 \dots g^{p-2}$ are all the nonzero residue classes mod p). Say we have $a \not\equiv 0$ mod p. We know $a \equiv g^k$ for some k ($0 \leq k \leq p-2$) - k is called the **index** or the **discrete log** of a to the base g mod p. This is a computationally hard problem, and is also used in cryptography.

Index Calculus - Let's say we're trying to solve a congruence $x^d \equiv 1$ mod p. Any x which satisfied this congruence is coprime to p. So if g is a primitive root

mod p, we can write $x \equiv g^k \bmod p$. New variable is now k:

$$\begin{aligned} x^u \equiv 1 \mod p &\longleftrightarrow g^{kd} \equiv 1 \mod p \\ &\longleftrightarrow p-1 = \operatorname{ord}(g) \text{ divides } kd \\ &\longleftrightarrow \frac{p-1}{(d,p-1)} \text{ divides } \frac{d}{(d,p-1)}k \\ &\longleftrightarrow \frac{(p-1)}{(d,p-1)} \text{ divides } k \end{aligned}$$

So set of solutions for k is exactly the set of multiples of $\frac{(p-1)}{(d,p-1)}$ (remember k is only modulo $p-1$). So we can get all the solutions x by raising g to the exponent k, where $0 \le k < p-1$ is a multiple of $\frac{p-1}{(d,p-1)}$. The number of solutions is

$$\frac{(p-1)}{\frac{p-1}{(d,p-1)}} = (d,p-1)$$

Similarly, if we're trying to solve the congruence $x^d \equiv a \bmod p$ ($a \not\equiv 0 \bmod p$), we can write $a \equiv g^l \bmod p$ so if $x \equiv g^k$ as before then $g^{kd} \equiv g^l \bmod p$. This means that $g^{kd-l} \equiv 1 \bmod p \leftrightarrow p-1|kd-l \leftrightarrow kd \equiv l \bmod p-1$ (k is variable), which has a solution iff $(d,p-1)$ divides l, in which case it has exactly $(d,p-1)$ solutions.

Note:

$$\begin{aligned} (d,p-1) \text{ divides } l &\longleftrightarrow p-1 \text{ divides } \frac{l(p-1)}{(d,p-1)} \\ &\longleftrightarrow g^{l\frac{p-1}{(d,p-1)}} \equiv 1 \mod p \\ &\longleftrightarrow a^{\frac{p-1}{(d,p-1)}} \equiv 1 \mod p \end{aligned}$$

Theorem 38. *There's a primitive root mod m iff $m = 1, 2, 4, p^e$, or $2p^e$ (where p is an odd prime). Let's assume that p is an odd prime, and $e \ge 2$. Want to show that there's a primitive root mod p^e.*

Part 1 - There's a primitive root mod p^2

Proof. Choose g to be a primitive root mod p, and use Hensel's Lemma to show there's a primitive root mod p^2 of the form $g+tp$ for some $0 \le t \le p-1$. We know $(g+tp,p) = 1$ since $p \nmid g$ and $p|tp$. $\operatorname{ord}_{p^2}(g+tp)$ must divide $\phi(p^2) = p(p-1)$.

On the other hand, if $(g+tp)^k \equiv 1 \bmod p^2$ then $(g+tp)^k \equiv 1 \bmod p \Leftrightarrow g^k \equiv 1 \bmod p \Leftrightarrow p-1|k$.

So $p-1$ divides $\operatorname{ord}_p(g+tp)$. Since $\operatorname{ord}_p(g+tp)$ is a multiple of $p-1$ and divides $p(p-1)$, it's either equal to $p-1$ or equal to $p(p-1) = \phi(p^2)$. We'll show that there's exactly one value of t for which the former happens.

Since there are p possible values of $t(0 \le t \le p-1)$, any of these remaining ones give a $g+tp$ which is a primitive root mod p^2. Consider $f(x) = x^{p-1} - 1$: mod p it has the root g. Since $f'(x) = (p-1)x^{p-2}$ and $f'(g) = (p-1)g^{p-2} \not\equiv 0 \bmod p$, by Hensel's Lemma there is a unique lift $g+tp$ of g mod p^2 satisfying $x^{p-1} \equiv 1$ mod p^2. This is the unique lift for which order is $p-1$ mod p^2. This proves that there's a primitive root mod p^2. □

Part 2 - Let g be a primitive root mod p^2. Then g is a primitive root mod p^e for every $e \ge 2$.

Proof. Since $\operatorname{ord}_{p^e}(g)$ divides $\varphi(p^e) = p^{e-1}(p-1)$ and also that $p-1 | \operatorname{ord}_{p^e}(g)$ (as in proof of previous part), $\operatorname{ord}_{p^e}(g)$ must be $p^k(p-1)$ for some $0 \le k \le e-1$. We want to show that $k = e-1$. To see that, it's enough to show that $g^{p^{e-2}(p-1)} \not\equiv 1$ mod p^e.

We'll show it by induction (base case is $e=2$). $g^{p-1} \not\equiv 1 \bmod p^2$ is true because g is a primitive root mod p^2, so order $= p(p-1)$. So say we know it for e.

We know that $\phi(p^{e-1}) = p^{e-2}(p-1)$. So $g^{\phi(p^{e-1})} \equiv 1 \bmod p^{e-1}$ assuming that $g^{\phi(p^{e-1})} \not\equiv 1 \bmod p^e$. In other words $g^{\phi(p^{e-1})} = 1 + bp^{e-1}$ with $p \nmid b$. Need to show it for $e+1$ - ie., $g^{\phi(p^e)} \not\equiv 1 \bmod p^{e+1}$.

We know that $g^{p^{e-2}(p-1)} = 1 + bp^{e-1}$. Raising to power p we get

$$\begin{aligned} g^{p^{e-1}(p-1)} &= (1+bp^{e-1})^p \\ &= 1 + pbp^{e-1} + \binom{p}{2}(bp^{e-1})^2 + \binom{p}{3}(bp^{e-1})^3 + \dots \\ &\equiv 1 + bp^e \mod p^{e+1} \end{aligned}$$

(because for $e \ge 2$, $3e-3 \ge e+1$ and $p | \binom{p}{2}$ so $\binom{p}{2} b^2 p^{2e-2}$ divisible by p^{2e-1} and $2e-1 \ge e+1$).

So $g^{p^{e-1}(p-1)} \equiv 1 + bp^e \bmod p^{e+1}$ with $p \nmid b$, which $\not\equiv 1 \bmod p^{e+1}$. Completes the induction. □

Main Proof. Check 1, 2, 4 directly. p odd, $m = p^e$ proved. $m = 2p^e$ (p odd) - $\phi(m) = \phi(2)\phi(p^e) = \phi(p^e)$. Let g be a primitive root mod p^e. If g is odd, it is a primitive root mod m. If not odd, then add p^e to it.

Now show that nothing else works: otherwise, if $n = mm'$ with m and m' coprime and $m, m' > 2$, we'll show there does not exist a primitive root mod m. By hypothesis ($m, m' > 2$) we know $\phi(m)$ and $\phi(m')$ are even. So for $(a, n) = 1$,

we have $(a, m) = 1 = (a, m')$. So $a^{\phi(m)} \equiv 1 \bmod m$ and $a^{\phi(m')} \equiv 1 \bmod m'$. So

$$\begin{aligned} a^{\phi(m)\phi(m')/2} &\equiv (a^{\phi(m)})^{\phi(m')/2} \\ &\equiv 1 \mod m \\ a^{\phi(m)\phi(m')/2} &\equiv 1 \mod m' \\ \text{Similarly so, } a^{\phi(m)\phi(m')/2} &\equiv 1 \mod n \end{aligned}$$

but $\phi(n) = \phi(m)\phi(m')$ so $\mathrm{ord}_n(a) < \phi(n)$. So a can't be a primitive root mod n.

Only remaining candidate is $n = 2^k$ for $k \geq 3$. No primitive root mod 8 since $\text{odd}^2 \equiv 1 \bmod 8$ (and $\phi(8) = 4$). So if a is odd, $a^2 = 1 + 8k$. Show by induction that $a^{2^{k-2}} \equiv 1 \bmod 2^k$ ($k \geq 3$). Since $\phi(2^k) = 2^{k-1}$, we see there does not exist a primitive root mod 2^k.

■

18.781 Theory of Numbers
Spring 2012